REMARKS

Claims 1-21 are pending in the application.

Claims 1-5 and 12-15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Number 4,969,190 to Takaragi, et al. ("Takaragi"), in view of U.S. Patent Number 5,432,849 to Johnson, et al. ("Johnson").

Claims 6-11 and 16-21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Takaragi in view of Johnson and in further view of *Applied Cryptography Second Edition, 1996* by Bruce Schneier ("Schneier").

Claims 1-6 recite a method of *enhancing throughput* of a pipelined encryption/decryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the method comprising the steps of: receiving a source datablock for a given stage and encryption/decryption context identifier; indexing according to the encryption/decryption context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, *the bank comprising a plurality of initial variables for each encryption/decryption context identifier*; and generating an output datablock from the source datablock and its corresponding initial variable. Claims 12-16 recite a *pipelined* encryption/decryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the encryption/decryption engine comprising: means for receiving a source datablock for a given stage and encryption/decryption context identifier; means for indexing according to the encryption/decryption context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, *the bank comprising a plurality of initial*

variables for each encryption/decryption context identifier; and means for generating an output datablock from the source datablock and its corresponding initial variable. Applicants respectfully submit that the exemplary features of Claims 1-6 and 12-16 have not been found to be taught or suggested in any of the aforementioned applied references, or any combination thereof.

As to claims 1 and 12, Takaragi teaches a specific method of implementing an algorithm with RSA characteristics using a Cipher Block Chaining (CBC) system. However, Takaragi does not teach a method of enhancing the throughput of a pipelined encryption/decryption engine. The specific problem of implementing CBC using RSA is that RSA uses a condition as a prerequisite in which only the data of the number smaller than a predetermined numerical value N can be encrypted. The feedback function in CBC (Takaragi, Figs. 1 and 2) can result in a number that exceeds the numerical value N, so that the input data cannot be correctly encrypted or decoded. In other words, Takaragi teach a method of calculating a number larger than the encryption block can handle. The present invention teaches an implementation of the CBC system that can keep a multistage pipelined encryptor engine operating at full capacity, thereby enhancing throughput (Paragraphs 6 and 19). The present invention enables encryption/decryption of data with a number that can exceed N. In fact, Takaragi does not even address the issue of keeping a multistage pipelined encryptor operating at its full information processing potential. Standard CBC mode requires the first data to clear the crypto block before the next piece of data from the same context may enter the crypto block, due to the standard feedback mechanism. Therefore, one would have to wait N cycles of the crypto block (N being the number of stages) before entering subsequent data. Using the

methods taught by Takaragi, the data still has to pass fully through all of the multiple stages of the block encryptor before being fed back into the mixing function at the input. The present invention can enable new data to enter the crypto block before previously entered data has fully passed through all of the stages. For these reasons, Applicants respectfully submit that Takaragi, alone or in combination with any of the aforementioned references, does not teach or suggest the exemplary features of the present invention. Claims 2-6 and 13-16, depend from claims 1 and 12, respectively. Therefore, Applicants respectfully submit that claims 1-6 and 12-16 are allowable and notice to that effect is requested.

Further to claims 1 and 12, the Examiner has correctly noted that Takaragi does not explicitly teach having a plurality of initial vectors or variables. The Examiner then supplied Johnson, stating that Johnson discloses a set of predetermined control vectors. Applicants respectfully submit that the full extent of Johnson's teaching is a method of generating control vectors internal to a cryptographic facility. The present invention teaches methods to deliver the crypto variables to the crypto engine at the right time in order to process data through the multiple pipeline stages without having to clear the stages when the context is changed. Johnson does not teach how to use cryptographic variables, such as initial vectors and keys, in order to keep the pipeline of a crypto block fully filled, thereby enhancing throughput. For these reasons, Applicants respectfully submit that Takaragi, alone or in combination with Johnson or any of the aforementioned references, does not teach or suggest the exemplary features of the present invention. Claims 2-6 and 13-16, depend from claims 1 and 12, respectively. Therefore, Applicants

respectfully submit that claims 1-6 and 12-16 are allowable and notice to that effect is requested.

As to claims 6-11 and 16-21, claims 6 and 16 depend from claims 1 and 12 and are therefore allowable for the reasons set forth above. Claims 7-11 recite a method of *enhancing throughput* of a pipelined encryption/decryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the method comprising: for each of a plurality of encryption/decryption contexts, *a number of which equals or exceeds the predetermined number of stages*, receiving a source datablock for the corresponding encryption context identifier; for each of the plurality of encryption/decryption contexts, indexing according to the encryption/decryption context identifier into a bank of variables comprising initial variables for the source datablock; and for each of the plurality of encryption/decryption contexts, generating an output datablock form the source datablock and its corresponding seed variable; wherein each stage of the pipelined encryption/decryption engine at any given time is processing source datablock from an encryption/decryption context different than encryption/decryption contexts of source datablocks being processed in all other stages of the pipelined encryption/decryption engine. Claims 17-21 recite an encryption/decryption engine *for enhancing throughput* of a pipelined encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, comprising: means for, as to each of a plurality of encryption/decryption contexts, *a number of which equals or exceeds the predetermined number of stages*, receiving a source datablock for the corresponding encryption context identifier; means for, as to each of the plurality of encryption/decryption contexts,

indexing according to the encryption/decryption context identifier into a bank of variables comprising initial variables and prior-stage output datablock to retrieve a seed variable for the source datablock; and means for, as to each of the plurality of encryption/decryption contexts, generating an output datablock from the source datablock and its corresponding seed variable; wherein each stage of the pipelined encryption/decryption engine at any given time is processing source datablocks from an encryption/decryption context different than encryption/decryption contexts of source datablocks being processed in all other stages of the pipelined encryption/decryption engine. Applicants respectfully submit that the exemplary features of Claims 7-11 and 17-21 have not been found to be taught or suggested in any of the aforementioned applied references, or any combination thereof.

As to claims 7 and 17, for the exemplary reasons set forth above with reference to claims 1-6 and 12-16, Applicants respectfully submit that Takaragi, alone or in combination with Johnson or any of the aforementioned references, does not teach or suggest the exemplary features of the present invention. The addition of Schneier does not cure the deficiencies of Takaragi, alone or in combination with Johnson or any of the aforementioned references. Schneier merely describes the cryptoanalysis of an algorithm called "FEAL." For these reasons, Applicants respectfully submit that Takaragi, alone or in combination with Johnson and/or Schneier or any of the aforementioned references, does not teach or suggest the exemplary features of the present invention. Claims 8-11 and 18-21, depend from claims 7 and 17, respectively. Therefore, Applicants respectfully submit that claims 7-11 and 18-21 are allowable and notice to that effect is requested.

In view of the foregoing, Applicant respectfully submits that Claims 1-21 are allowable and requests notice to that effect.

Further and favorable consideration is respectfully requested.

Respectfully submitted,

Date: 03/16/05

Madelynne J. Farber
Registration No. 45,410

Sandia National Laboratories
P.O. Box 5800, MS 0161
Albuquerque, NM 87185-0161
(p) 505-844-3858, (f) 505-844-9955